

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA**

IN THE MATTER OF THE SEARCH OF)	Case No. 1:19-mj-00026-MMS
)	
Black Samsung DUOS cellphone, serial)	<u>UNDER SEAL</u>
number RF8K51P5Q5K)	
)	
)	
)	

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, Matthew B Judy, being first duly sworn, upon oath, depose and state the following:

BACKGROUND

1. I am currently employed as a Special Agent (SA) for the Federal Bureau of Investigation (FBI), and have been so employed since August of 2004. During my employment with the FBI, I have been assigned the investigation of criminal matters within the jurisdiction of the FBI, with emphasis in the areas of violent crimes, which includes the investigations of crimes against children, and violent criminal enterprise investigations. In addition to my current assignment, I have served in Utah and along the United States-Mexico border of Texas. In both previous locations, I was tasked to investigate violent crimes, including crimes against children, and violent criminal enterprises among other crimes. I am currently assigned to the Juneau Resident Agency within the Anchorage Division of the FBI and have been so assigned since October of 2010.



AUG 09 2019

Page 1 of 45

2. In my current position, I am responsible for, among other things, conducting investigations that involve, but are not limited to, crimes on the high seas, violent criminal enterprises, violent incident crimes, crimes against children, and drug trafficking.

3. Due to the proliferation of technical resources in criminal activity, particularly the use of computers, smart phones, and other digital devices, I have investigative experience with technical aspects of criminal investigations and I have attended trainings, conferences, and seminars that have provided me training on technical resources.

4. The information contained in this affidavit is derived from my own personal knowledge and experience, and from other law enforcement and non-law enforcement personnel.

5. This investigation concerns allegations of violation of 18 U.S.C. § 1801, Video Voyeurism; § 2251(a), Production of Child Pornography; § 2252(a)(1), Transportation of Child Pornography; and § 2252(a)(4)(B), Possession of Child Pornography.

PROPERTY TO BE SEARCHED

6. This affidavit is made in support of an application for a warrant to search a black Samsung DUOS cellphone, serial number RF8K51P5Q5K, hereinafter referred to as the SUBJECT DEVICE and described in Attachment A (attached hereto and incorporated herein by this reference). The SUBJECT DEVICE was released to the FBI

Page 2 of 45



AUG 09 2019

by the security officer of the cruise ship (C/S) Royal Princess on August 7, 2019. The SUBJECT DEVICE was released to the FBI while the ship was secured to the dock in Skagway, Alaska, and is currently in the custody of the FBI at the Juneau Resident Agency of the FBI, located at 709 West 9th Street, Room 957, Juneau, Alaska.

7. Since this affidavit is being submitted for the limited purpose of securing a warrant to search and seize the items specified in Attachment B (attached hereto and incorporated herein by this reference), which constitutes evidence, fruits or instrumentalities of violations or attempted violations of 18 U.S.C. § 1801, § 2251(a), §2252(a)(1), and § 2252(a)(4)(B) from the aforementioned property, I have not included each and every fact known to me regarding this investigation. I have set forth only the facts that I believe are necessary to establish a foundation for the requested search warrant.

8. The relevant statutory authority and terms used in this affidavit and its attachments are described and defined below.

RELEVANT STATUTES

9. The following statutes are relevant to this application:

- a. 18 U.S.C. § 1801 provides, in relevant part, that whoever, in the special maritime and territorial jurisdiction of the United States, has the intent to capture an image of a private area of an individual without their consent, and knowingly does so under circumstances in which the individual has a reasonable expectation of privacy, shall



AUG 09 2019

be fined under this title or imprisoned not more than one year, or both.

- b. 18 U.S.C. § 2251(a) provides, in relevant part, Any person who employs, uses, persuades, induces, entices, or coerces any minor to engage in, or who has a minor assist any other person to engage in, or who transports any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, shall be punished as provided under subsection (e), if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed.



AUG 09 2019

- c. 18 U.S.C. § 2252(a)(1) provides, in relevant part, any person who knowingly transports or ships using any means or facility of interstate or foreign commerce or in affecting interstate or foreign commerce by any means including by computer or mails, any visual depiction, if – (A) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and (B) such visual depiction is of such conduct.
- d. 18 U.S.C. § 2252(a)(4)(B) provide, in relevant part, that any person who knowingly possesses, or knowingly accesses with intent to view any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been so transported, by any means including by computer, if (i) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and (ii) such visual depiction is of such conduct, or any person who attempts to do so, shall be guilty of a federal offense.

DEFINITIONS

10. The following terms are relevant to this affidavit in support of this application for a search warrant:

1:19-mj-00026-MMS

Page 5 of 45



AUG 09 2019

- a. *Capture*: With respect to an image, means videotape, photograph, film, record by any means, or broadcast. *See* 18 U.S.C. § 1801(b)(1)
- b. *Child Erotica*: The term “child erotica” means any material relating to minors that serves a sexual purpose for a given individual, including fantasy writings, letters, diaries, books, sexual aids, souvenirs, toys, costumes, drawings, and images or videos of minors that are not sexually explicit.
- c. *Child Pornography*: The term “child pornography” is defined at 18 U.S.C. § 2256(8). It consists of visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct. *See* 18 U.S.C. §§ 2252 and 2256(2), (8).
- d. *Minor*: The term “minor” means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).



AUG 09 2019

- e. *Private Area of Individual*: As used in 18 U.S.C. § 1801(a), the term means the naked or undergarment clad genitals, pubic area, buttocks, or female breast of that individual. *See* 18 U.S.C. § 1801(b)(1)
- f. *Sexually Explicit Conduct*: The term “sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. *See* 18 U.S.C. § 2256(2).
- g. *Under Circumstances in Which That Individual has a Reasonable Expectation of Privacy*: As used in 18 U.S.C. § 1801(a) means (A) circumstances in which a reasonable person would believe that he or she could disrobe in privacy, without being concerned that an image of a private area of the individual was being captured; or (B) circumstances in which a reasonable person would believe that a private area of the individual would not be visible to the public, regardless of whether that person is in a public or private place. *See* 18 U.S.C. § 1801(b)(1).
- h. *Visual Depictions*: “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic



AUG 09 2019

means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

11. The following technical terms are relevant to my affidavit in support of this application for a search warrant.

- a. As part of my training, I have become familiar with the Internet (also commonly known as the World Wide Web), which is a global network of computers¹ and other electronic devices that communicate with each other using various means, including standard telephone lines, high-speed telecommunications links (e.g., copper and fiber optic cable), and wireless transmissions including cellular networks and satellite. Due to the structure of the Internet, connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via electronic mail ("e-mail").

¹ The term "computer" is defined by 18 U.S.C. § 1030(e)(1) to mean "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device."



AUG 09 2019

b. Set forth below are an alphabetical listing of some definitions of technical terms, used throughout this Affidavit, and in Attachments A and B, hereto, pertaining to the Internet and computers more generally.


i. Compressed file: A “compressed file” is a file that has been reduced in size through a compression algorithm to save disk space. The act of compressing a file will make it unreadable to most programs until the file is uncompressed.

ii. Computer system and related peripherals, and computer media: As used in this Affidavit, the terms “computer system and related peripherals, and computer media” refer to tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drives and other computer-related operation equipment, digital cameras, scanners, in addition to computer photographs, and other visual depictions of such graphic interchange formats, including but not limited to, JPG, GIF, TIF, AVI, and MPEG.




AUG 09 2019

- iii. Digital device: A “digital device” includes any electronic system or device capable of storing and/or processing data in digital form, including central processing units; desktop, laptop or notebook computers; tablets, internet-capable cellular phones (smart phones), or personal digital assistants; wireless communication devices such as telephone paging devices, beepers, and mobile telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices such as modems, cables, and connections; storage media such as hard disk drives, flash drives, thumb drives, floppy disks, compact disks, DVDs, magnetic tapes, and memory chips; and security devices.
- iv. Hash value: A “hash value” is a mathematical algorithm generated against data to produce a numeric value that is representative of that data. A hash value may be run on media to find the precise data from which the value was generated. Hash values cannot be used to find other data. The term “SHA-1” or “SHA-1 hash” refers to a type of hash value that may be given to a computer file. The SHA-1 is a cryptographic hash function designed by the United States


AUG 09 2019

National Security Agency and is a United States Federal Information Processing Standard. SHA stands for “secure hash algorithm.” SHA-1 hash value is the standard for unique identifying numbers. It is computationally infeasible for two files with different content to have the same hash values. I am unaware of any instance in which two files have been naturally assigned the same SHA-1 hash value.

- v. Image or copy: An “image or copy” is an accurate reproduction of information contained on an original physical item, independent of the electronic storage device. “Imaging” or “copying” maintains contents, but attributes may change during the reproduction.
- vi. Log files: “Log files” are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a web site was accessed by remote computers; access logs list specific information about when a computer was accessed from a


AUG 09 2019

remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

vii. Malicious Software (“malware”): Software designed to infiltrate a computer without the owner’s informed consent is called “malicious software” or “malware.” The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. Software is considered malware based on the perceived intent of the creator rather than any particular features. Malware includes computer viruses, worms, Trojan horses, most rootkits, spyware, dishonest adware, and other malicious and unwanted software.

viii. Metadata: “Metadata” are data contained in a file that is not usually associated with the content of a file but is often associated with the properties of the application or device that created that file. For example, a digital camera photograph often has hidden data that contains information identifying the camera that manufactured it and the date the image was taken.

ix. Steganography: “Steganography” is the art and science of communicating in a way that hides the existence of the



AUG 09 2019

communication. Within the computer world, It can be used to hide a file inside another. For example, a child pornography image can be hidden inside another graphic image file, audio file, or other file format.

- c. The terms "*records*" and "*information*" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writings, drawings or paintings); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

COMPUTERS AND CHILD PORNOGRAPHY

12. Based upon my training and experience as well as my discussions with others involved in child pornography investigations, computers and computer technology have revolutionized the way in which child pornography is produced, distributed, received and possessed.

13. Through the use of computers and the Internet, distributors of child pornography use various distribution networks, including but not limited to, personal email contacts, file-sharing services, list serves, and membership-based/subscription-based web sites to conduct business, allowing them to remain relatively anonymous.



AUG 09 2019

14. The development of computers has also revolutionized the way in which child pornography collectors interact with each other, and sexually exploit children. Computers serve four basic functions in connection with child pornography: production, communication and distribution, and storage. More specifically, the development of computers has changed the methods used by child pornography collectors in these ways:

- a. *Production:* Producers of child pornography can now produce high resolution still and moving images directly from a common video or digital camera, to include cellphones with built in cameras. In this day and age, these types of cameras have become ubiquitous, and are located on nearly every cell phone sold. Once taken, images and videos can be saved onto a computer or uploaded onto a website or attached to an email within seconds. While still on the camera or after being saved onto a computer or uploaded into a photo or video editing program, images can be edited in ways similar to how a photograph may be altered. Images can be lightened, darkened, cropped, or otherwise manipulated. Videos can be edited, or spliced together to create montages of abuse that can be several minutes to several hours long. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the pornographer in that this method of production does not leave as



AUG 09 2019

large a trail for law enforcement to follow. In some cases, depending upon the sophistication of the producer, it may be virtually impossible to law enforcement to determine the source of a sexually explicit image.

- b. *Communication and Distribution:* The Internet allows any computer to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. In addition, the Internet allows users, while still maintaining anonymity, to easily locate (i) other individuals with similar interests in child pornography; and (ii) web sites that offer images of child pornography. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions between child pornography collectors over the Internet. Sometimes the only way to identify both parties and verify the transportation of child



AUG 09 2019

pornography over the Internet is to examine the recipient's computer to look for "footprints" of the web sites and images accessed by the recipient.

- c. *Storage:* The computer's capability to store images in digital form makes it an ideal repository for child pornography. It is not uncommon to cellphones with 32 gigabytes (GB) or more of data. Many cellphones also have expandable external storage in the form of SD cards or other storage devices. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 1 terabyte are not uncommon. These drives can store thousands of images at very high resolution. Storage options located outside the physical boundaries of a computer add another dimension to the equation. According to www.avforums.com, 1 GB of data equates to approximately 20 minutes of high definition video.
- d. Child pornographers can now transfer photographs onto a computer directly from a digital camera, cellphone, or from a regular camera by using a scanner. A computer's electronic storage media (commonly referred to as the hard drive) can store tens of thousands of images at a very high resolution. In addition, magnetic storage



AUG 09 2019

located in host computers makes it possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image in another country. Once done, there is no readily apparent evidence at the "scene of the crime." Only careful laboratory examination of electronic storage devices can recreate the evidence trail.

15. Collectors and distributors of child pornography can set up an account with a remote computing service that provides e-mail services and electronic file storage. Evidence of such online storage of child pornography may be found on the user's computer.

16. Information can be saved or stored on a computer intentionally. For example, a person may save an e-mail as a file or may save a favorite website in a "bookmark" type file. Information can also be retained unintentionally. For example, traces of an electronic communication path may be stored automatically in temporary files or Internet Service Provider client software. In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Internet distributors and recipients of child pornography may be identified by examining the recipient's computer, including the Internet history and cache to look for "footprints" of the websites and images accessed by the recipient. A forensic examiner often also can recover



AUG 09 2019

evidence suggesting whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded.

17. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive or viewed via the Internet. Even when such files have been deleted, they can often be recovered by forensic tools. When a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside for long periods of time in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space (free space or slack space). In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits.

ITEMS TO BE SEIZED

18. The following items to be seized constitute contraband, fruits, instrumentalities, and evidence of violations, or attempted violations, of 18 U.S.C. §§



AUG 09 2019

1801, 2251(a), 2252(a)(1), and 2252(a)(4)(B) relating to the crimes of video voyeurism and production, possession, and transportation of visual depictions of minors engaging in sexually explicit conduct and child pornography:

- a. Child pornography;
- b. Child erotica;
- c. Visual depictions of minors engaged in sexually explicit conduct;
- d. Images or video recordings of adults or children with the appearance that they were made without consent and under circumstances in which the individual appears to have a reasonable expectation of privacy;
- e. Information, correspondence, records, documents or other materials constituting evidence of or pertaining to video voyeurism, child pornography, child erotica, or visual depictions of minors engaged in sexually explicit conduct; or constituting evidence of or pertaining to video voyeurism, or the production, possession, or transportation through interstate or foreign commerce of child pornography, child erotica, or visual depictions of minors engaged in sexually explicit conduct; or constituting evidence of or pertaining to an interest in video voyeurism, child pornography or sexual activity with children;
- f. Records or documents evidencing ownership or use of the SUBJECT DEVICE;

A handwritten signature in black ink, appearing to be a stylized 'J' or 'G' with a loop at the bottom.

AUG 09 2019

- g. Evidence or records of who used, owned, or controlled the SUBJECT DEVICE at the time the things described in this warrant were created, edited, or deleted;
- h. Evidence of the times the SUBJECT DEVICE was used;
- i. Records of or information about the DEVICE's Internet activity, including Internet Protocol addresses used by the DEVICE.

PROBABLE CAUSE

19. On August 7, 2019, at approximately 11:30 AM, FBI SA Matthew Judy received a telephone call from a Holland America Group Marine Security Investigations Manager. SA Judy was told that a 27-year-old female passenger on board the C/S Royal Princess had reported on August 6, 2019, that she had been the victim of video voyeurism.

20. The female victim indicated that between approximately 8:30 AM and 8:45 AM, she entered a door to the bathroom area of deck five, located midship on the portside. Inside the first door were three other doors, one to a woman's bathroom, one to a man's bathroom, and one to a disabled ADA compliant bathroom. As she passed through the door, a male crewmember with a nametag bearing the name "Richard" was inside. He indicated that she should use the ADA bathroom because it was clean. She entered the ADA bathroom and utilized the toilet.



AUG 09 2019

21. While in the bathroom, she noticed a box containing cleaning materials, bottles and cloths, on the floor. She looked closer at the box and discovered a mobile telephone in the box with the camera facing towards the toilet. The telephone was partially covered by cleaning cloths. She picked the telephone up and noticed the screen was lit up and the video recorder was turned on. The recorder had been recording for approximately five minutes. She stopped the recording and played the first approximately three seconds of the video. She observed Richard on the video arranging the phone in the bathroom.

22. The female exited the bathroom and confronted Richard. She asked why he was recording and he asked her not to tell anyone because he would lose his job. Richard attempted to grab the phone from the female. The female made Richard delete the video and then delete the video from the deleted folder. Richard complied with her request. The female then suggested that they check elsewhere on the phone to make sure there were no other locations where the video was stored. After this request, Richard took the phone and left the area. The female then reported the incident to the Guest Services Desk. The female indicated she wanted the ship's senior management to deal with the incident and she did not want law enforcement involved.

23. C/S Royal Princess security personnel located Richard, identifying him as Richard Harvey Olipano Magbanua, a Philippine citizen. Security personnel conducted a search of Magbanua's cabin, cabin number 33011, in accordance with their internal

A handwritten signature in black ink, appearing to be a stylized 'M' or 'W' followed by a loop.

AUG 09 2019

policies. Security personnel intended to investigate the incident as an administrative matter and to terminate Magbanua if the allegations were true.

24. On August 6, 2019, Security personnel seized the SUBJECT DEVICE, a black Samsung DUOS cellphone, serial number RF8K51P5Q5K, from Magbanua's cabin and interviewed Magbanua. Magbanua advised that among other duties, he was assigned to clean and look after the Deck Five and Deck Six guest toilets. He advised that at approximately 9:45 AM, he was cleaning the ADA toilet on Deck Five when a female guest asked to use the toilet he was cleaning. Magbanua left the bathroom so that she could use the bathroom, but left his cleaning trolley inside the bathroom. At the time, Magbanua had been using his mobile telephone to download updates and the screen was on. The guest saw the phone and thought Magbanua was recording her. He immediately took his telephone to his cabin, because he knew he would be in trouble for using the telephone in a guest area. Magbanua stated that he was not videotaping the guest as she suggested.

25. Royal Princess Information Technology (IT) personnel were requested by ship security to search the telephone in order to determine who was telling the truth. IT personnel loaded multiple software programs onto the telephone in order to recover deleted files. One of the programs, MobiSaver, was able to recover some deleted files, to include video and still images. Neither IT personnel nor security personnel reviewed the entire telephone.



AUG 09 2019

26. Security personnel reviewed some of the images and videos from the SUBJECT DEVICE and discovered still images of women in what appeared to be the Deck Five ADA bathroom. The images included a number of different women, at various stages of using the bathroom. Some women were clothed and some had the clothing covering their lower bodies removed. Security personnel advised that in addition to adult women, there were some images of girls who appeared to be under the age of 18. Some images captured the uncovered vagina and buttocks area of women. There were also videos taken outside of the bathroom area where the camera appeared to be near ground level and angled upward. The video captured images looking up dresses and skirts of women.

27. On August 7, 2019, before contacting law enforcement, security personnel re-interviewed Magbanua and told him that they had found video clips where Magbanua had covertly videoed guests and crew in the toilets and work place. In response, Magbanua advised that he had taken the videos without the knowledge or consent of the women being viewed. Magbanua approximated that he had created videos of at least 20 women, some old and some young. Magbanua advised that he had also taken screen shots of the videos he had taken. Magbanua further advised that he had been making videos since May 2019. He knew it was wrong, but could not help himself.

28. On August 7, 2019, at approximately 2:30 PM, SA Judy boarded the C/S Royal Princess in order to conduct an investigation.



AUG 09 2019

29. Royal Princess security personnel provided SA Judy with digital copies of the images and videos they had discovered on Magbanua's telephone. Security advised that not all images or videos on the telephone were reviewed nor downloaded. The video of the female victim who reported the incident on August 6, 2019 had not been recovered by Royal Princess IT. Security provided SA Judy with 10 videos, 40 still images that had been recovered by MobiSaver, and 22 images associated with Facebook and crewmembers from the Royal Princess.

30. SA Judy reviewed the images provided by ship security. At least 18 different females could be seen in the images. It is unclear if the females are minors, but three appeared to be under the age of 18. The age determination was made solely on the physical appearance of the females, and SA Judy's estimation of their age.

31. One image appeared to be a screenshot of a video and showed a female who appeared to be under the age of 18 years old. The camera appeared to have been set up 90 degrees to the side of the toilet. The image depicts the female standing in front of the toilet, turned so she is facing the camera. The female's pants are pulled down to her knees, exposing the vaginal and pubic areas, which were visible to the camera. It is unclear if the female is a minor, because the age determination was an approximation made by SA Judy based upon the appearance of the female's face and what appeared to be minimal pubic hair growth.

32. Two still images reviewed by SA Judy depicted a female who wore a crew member uniform. The camera appeared to have been set up 90 degrees to the side of the



AUG 09 2019

toilet and both images depict the female sitting on the toilet, with her bare thigh area and side of buttocks area visible to the camera.

33. Royal Princess security personnel were able to identify the female crewmember and requested that she speak with SA Judy. SA Judy interviewed the crewmember and she identified herself in the images. She was unaware that she had been videoed and did not give consent for the videos to be taken. She expected the bathroom to be private. The crewmember identified the bathroom as most likely being the bathroom on deck five.

34. On August 7, 2019, SA Judy interviewed Magbanua. Before conducting an interview, SA Judy read Magbanua his Miranda Rights. Magbanua stated that he understood and was willing to speak to SA Judy.

35. During the interview with Magbanua, he advised that he had used his cellular telephone to make videos of women in the bathroom and outside of the bathroom. He created the videos without the knowledge or consent of the women. Magbanua made videos of women of all ages, to include young women, but he was not sure if any of them were under 18 years of age. Magbanua stated that after he was confronted by the female on August 6, 2019, he deleted all of the videos he had made inside of the bathroom.

36. SA Judy showed Magbanua the images that Royal Princess security had removed from Magbanua's telephone. Magbanua advised that he had created all of the videos. He stated that the still images were actually videos. He believed that when the



AUG 09 2019

videos were recovered, the software only recovered a single frame of the videos. Of all the still shots in the bathroom that SA Judy showed to Magbanua, he identified only one as being a screenshot that he had created himself from a video. The screenshot was identified by Magbanua because there was a volume bar on the top of the image. Magbanua advised that this was the only image where Magbanua made a screen shot image from a video. The image he identified as being a screenshot he created was the image of the female who appeared to be a minor that is described in paragraph 31 above.

37. Magbanua was shown the SUBJECT DEVICE, which Magbanua identified as his telephone and that it was the telephone utilized to create the videos and images that were the subject of the interview.

JURISDICTIONAL MATTERS

38. The C/S Royal Princess is a cruise ship operated by Princess Cruise Lines. During the summer season of 2019, the ship has conducted Alaska cruises since May 2019. The ship has maintained Alaskan cruise itineraries from May 2019 until the present. The ship maintains itineraries that take it from Vancouver, British Columbia, Canada, through Southeast Alaska destinations, to Whittier, Alaska. The ship then turns around and travels from Whittier, Alaska through Southeast Alaska destinations, to Vancouver, British Columbia, Canada. The Royal Princess has repeated the above described itineraries through the summer. Each leg (One leg being Vancouver to Whittier, the other leg being Whittier to Vancouver) takes approximately one week to complete.



AUG 09 2019

39. The "Special Maritime and Territorial Jurisdiction of the United States" is defined in 18 U.S.C., Section 7. 18 U.S.C. Section 7(1) and (8) defined the term to include, "[t]he high seas, any other waters within the admiralty and maritime jurisdiction of the United States and out of the jurisdiction of any particular State..., " as well as, "any foreign vessel during a voyage having a scheduled departure, from or arrival in the United States with respect to an offense committed by or against a national of the United States."

40. While underway, the Royal Princess passes through multiple maritime jurisdictions on the above described itineraries. The ship regularly transits between Alaskan waters and into the United States territorial Seas that are outside of Alaska, and then into international waters. At times, the vessel also transits through Canadian territorial seas.

41. The Royal Princess is a ship registered in Bermuda, which is a British Overseas Territory. The ship is owned by Princess Cruises, whose parent company is publicly traded in the United States of America.

42. The Royal Princess carries, on average, approximately 3,600 passengers and 1,350 crew. Passengers and crew are people of many nationalities, to include United States citizens.

43. Magbanua has been an employee on board the Royal Princess throughout the summer season in Alaska and has been on board the ship during all summer voyages. Magbanua has also had the SUBEJECT DEVICE with him during the summer voyages.



AUG 09 2019

Magbanua provided two time periods for when he was creating surreptitious videos in the bathroom on board the ship: He had stated that he had been doing it since May 2019 and he also made a statement that he had been making the videos for about a month.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

44. Searches and seizures of evidence from computers and other Internet access devices require agents to seize most or all electronic items (hardware, software, passwords and instructions) to be processed later by appropriate personnel in a controlled environment. Digital storage media may include but is not limited to floppy disks, hard drives, tapes, DVD disks, CD-ROM disks or other magnetic, optical or mechanical storage which can be accessed by computers or other electronic devices to store or retrieve data, which can store the equivalent of thousands of pages of information. Users may store information or images in random order with deceptive file names, which requires searching authorities to examine all the stored data to determine whether it is included in the search warrant. This sorting process renders it impractical to attempt this kind of data search on site.

45. Searching digital evidence systems for criminal evidence requires experience in the computer and cellular telephone field and a properly controlled environment in order to protect the integrity of the evidence and recover even "hidden," erased, compressed, password-protected, or encrypted files. Since digital evidence is extremely vulnerable to tampering or destruction (both from external sources and from



AUG 09 2019

destructive code imbedded in the system as a “booby trap”), a controlled environment is essential to its complete and accurate analysis.

46. As described above and in Attachment B, this application seeks permission to search and seize records that might be found in the digital devices, in whatever form they are found. One form in which the records might be found is that they are stored on a computer’s hard drive, or other electronic media. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis of the computer(s) or other electronic storage media seized.

47. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processor, picture, and movie files), computer hard drives can contain other forms of electronic evidence as well. In particular, records of how a computer has been used, the purposes for which it was used, and who has used it are called for by this warrant. As described above, data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs store configuration information on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record



AUG 09 2019

additional information, such as the attachment of peripherals (e.g., cameras and printers for creating or reproducing images), the attachment of USB flash storage devices, and the times and dates the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created. This information can sometimes be evidence of a crime, or can point toward the existence of evidence in other locations. Evidence of this type is a conclusion, based on a review of all available facts and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand the evidence described in Attachment B is included within the scope of the warrant.

48. In finding evidence of how a computer has been used, the purposes for which it was used, and who has used it, sometimes it is necessary to establish that a particular thing is not present on a drive. For example, I know from training and experience that it is possible that malicious software can be installed on a computer, often without the computer user's knowledge. This software can allow a computer to be used by others. To investigate the crimes described in this warrant, it might be necessary to investigate whether any such malicious software is present on the computer, and, if so, whether the presence of that malicious software might explain the presence of other things found on the computer's hard drive.

49. Law enforcement personnel trained in searching and seizing computer data will seize items of evidentiary value, and transport the same to an appropriate law enforcement laboratory for off-site review. The electronic media will be reviewed for the

A handwritten signature in black ink, appearing to be a stylized 'J' or 'G' followed by a loop.

AUG 09 2019

evidence described in Attachment B in accordance with and as defined by the review protocols described below.

50. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - for long periods of time before they are overwritten. Files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. The search for these files and file fragments can take considerable time, depending on the computer user's practices.

A handwritten signature in black ink, appearing to be 'WJ' followed by a large loop.

AUG 09 2019

51. I know from training and experience that computers or other digital devices used to access the Internet usually contain files, logs or file remnants which would tend to show ownership and use of the device, ownership and use of any external devices that had been attached to the computer or other digital devices, as well as ownership and use of Internet service accounts used for the Internet or cellular data network access.

SPECIFIC METHODS OF SEARCHING FOR DIGITAL EVIDENCE

52. I am seeking authority to search for, among other things, items containing digital data, more particularly described in Attachment B. Consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

53. The search of a computer hard drive or other computer storage medium is a time-consuming manual process often requiring months of work. This is so for a number of reasons, including the complexity of computer systems, the multiple devices upon which computing can take place, and the tremendous storage capacity of modern day computers, and the use of encryption or wiping software. As explained above, modern day computers and storage devices are capable of holding massive quantities of data, and



AUG 09 2019

the volume of evidence seized in these cases can be immense. I am aware of cases in which individuals have possessed thousands of images on their computer, multiple computers and hard drives, or dozens of storage media upon which contraband images were found. I know from my training and experience, and from my discussions with trained computer forensic examiners, that a review of such quantities of evidence can take a significant amount of time. Second, there is a limited pool of personnel capable of conducting a forensic examination. Third, in some instances an individual may utilize encryption software or other publically-available techniques such as wiping software to hide their digital activity. Forensic tools are available to circumvent some of these techniques; however, these tools may require a significant allocation of resources and a substantial period of time.

54. Some or all of the following search methods may be used to conduct the forensic search in this case. These methods are not listed in any particular order, nor is their listings in this affidavit a representation that they will be used in this particular case:

- a. *Keyword Searches:* I know that computer forensic utilities provide the capability for a user to search for specific key words that may exist on a piece of digital media. I intend to use specific keywords. As it concerns to the investigation described above, examples of such keywords include, but are not limited to "Divorce," and "Domestic violence." Those keyword searches will indicate files and other areas of the hard drive that need to be further reviewed to



AUG 09 2019

determine if those areas contain relevant data. A list of keywords utilized will be maintained with the records of the forensic examination.

- b. *Data Carving*: I know that, as previously mentioned, data residue may be left in the "free," "unallocated," or "slack" space of a computer hard drive, that is, the space not currently used by active files. I further know that, as previously mentioned, many operating systems utilize temporary storage often referred to as "swap space" on the hard drive to store contents from main system memory. Such unallocated and swap space may contain the residue of files that can be carved out, often in an automated or semi-automated fashion. I intend to use forensic tools to carve out files, in particular, image files such as JPEG and GIF files. The mere act of carving out such files does not expose me to the contents of such recovered files, but makes those files available for further relevancy checks, such as keyword searches (explained above) and hash value comparisons (explained below).
- c. *Hash Value Comparisons*: I know that computer forensic utilities provide the capability to utilize a function known as a hash algorithm. A hash algorithm uses a mathematical formula to analyze the data composing a file, and to generate a unique "fingerprint" for



AUG 09 2019

that file. The act of hashing a piece of data does not reveal to an investigator any information about the contents of that data.

However, I know that computer forensic applications often contain databases of known hash values for files. Some of those files are "ignorable," which enables other forensic processes to ignore files (such as the Windows operating system) that are not evidentiary in nature. I seek permission to utilize automated hash value comparisons to both exclude irrelevant files, and to potentially locate relevant files. Hash value comparisons are useful, but not definitive, as even a single-bit change to a file will alter the hash value for the file. The forensic review team does not intend to rely solely on hash value comparisons, but intends to utilize them in order to assist with identifying relevant evidence. The use of this search method is intended to narrow the search. A search of known hash values, however, will not be used exclusively because I know that typically there are many files on digital devices with unknown hash values. Using a hash value search method exclusively would not uncover the data as well as other evidence authorized by this warrant and described in Attachment B.

d. *Opening Container Files, Encrypted Volumes, and Embedded Files:*

I know that relevant data may be compressed, encrypted, or



AUG 09 2019

otherwise embedded in other files or volumes. It is often not possible through any automated process to examine the contents of such containers without opening them, just as it is not possible to examine the contents of a locked safe without first opening the safe. In the event that compressed, encrypted, or otherwise embedded files or volumes may exist on the seized items, I intend to request the use of sophisticated forensic tools to attempt to open any such container files that may reasonably contain evidence.

- e. *File Header / Extension Checks:* I know that individuals involved in illegal activities or attempting to hide activities from other users on a computer often change the extension of a file (such as .jpg) to some other incompatible extension (such as .txt) in order to disguise files from casual observers. An example of a person attempting to hide activities on a computer would be that of a domestic abuse victim attempting to hide documents related to assistance for victims. The extension of a file, however, is not necessarily linked to the "header" of a file, which is a unique marking imbedded automatically in many types of files. By comparing the extension of a file with the "header information" of a file, it is possible to detect attempts to disguise files. Such a comparison can be made in an automated process by computer forensic tools. I intend to run an automated header



AUG 09 2019

comparison to detect such efforts, and intend to review any such files that reasonably may contain evidence authorized by this warrant.

- f. *Thumbnail / Image Views*: Because the majority of the expected files will not have known hash values, a negative hash value comparison does not exclude a file. There is no known alternative for visually inspecting each file. I therefore intend to examine at least a thumbnail image of each image file on the digital media whether "live," "data carved," or identified by header as well as other files.
- g. *Registry / Log File Checks*: I know that it is necessary in any criminal case to establish not only that a crime has occurred, but also to establish what person committed that crime. Operating systems and computer programs often maintain various administrative files such as logs that contain information about user activities at certain times. In the Windows operating system, for example, some of these files are collectively referred to as "the registry". Such files contain specific information about users, often including e-mail addresses used, passwords stored, and programs executed by a particular user. These files may also contain evidence regarding storage devices that have been connected to a computer at some time. Multiple backup copies of such files may exist on a single computer. I intend to



AUG 09 2019

examine these files to attempt to establish the identity of any user involved in the creation, editing, or use of files found on the digital devices, and to establish methods (such as software used) and dates of this activity.

- h. *Metadata / Alternative Data Streams*: I know that many file types, operating systems, and file systems have mechanisms for storing information that is not immediately visible to the end user without some effort. Metadata, for example, is data contained in a file that is not usually associated with the content of a file, but is often associated with the properties of the application or device that created that file. For example, a digital camera photograph often has hidden data that contains information identifying the camera that manufactured it, and the date the image was taken. Some file systems for computers also permit the storage of alternate data streams, whereby a file such as a text file may hide an image file that would not be immediately visible to an end user without some action taken. I know that both metadata and alternative data streams may contain information that may be relevant. Metadata and alternative data streams are often identified and processed automatically by computer forensic utilities. I intend to review any such data that is flagged by any process above as being relevant.



AUG 09 2019

55. Criminal Procedure Rule 41 specifically states "The officer may retain a copy of the electronically stored information that was seized or copied." Fed. R. Crim. P. 41 (f)(1)(B). Moreover, upon identification of contraband, the item is subject to forfeiture, and the owner has a reduced expectation of privacy in those seized devices. Consequently, should a seized device be found during the authorized forensic review to contain contraband, it will be retained by the United States, and may be searched without further authorization of the Court for the evidence described in Attachment B. Such a later search may be required for the following reasons:

- a. Should the execution of the warrant uncover data that may later need to be introduced into evidence during a trial or other proceeding, the authenticity and the integrity of the evidence and the government's forensic methodology may be contested issues. Retaining copies of seized storage media may be required to prove these facts.
- b. Returning the original storage medium to its owner will not allow for the preservation of that evidence. Even routine use may forever change the data it contains, alter system access times, or eliminate data stored on it.
- c. Because the investigation is not yet complete, it is not possible to predict all possible defendants against whom evidence found on the storage medium might be used. That evidence might be used against persons who have no possessory interest in the storage media, or



AUG 09 2019

against persons yet unknown. Those defendants might be entitled to a copy of the complete storage media in discovery. Retention of a complete image assures that it will be available to all parties, including those known now and those later identified.

- d. The act of destroying or returning storage medium could create an opportunity for a defendant to claim, falsely, that the destroyed or returned storage medium contained evidence favorable to him. Maintaining a copy of the storage medium would permit the government, through an additional warrant if necessary, to investigate such a claim.
- e. Similarly, should a defendant suggest an explanation for the presence of evidence on storage medium or some defense, it may be necessary to investigate such an explanation or defense by, among other things, re-examining the storage medium with that explanation or defense in mind. This may require an additional examination of the storage medium for evidence that is described in Attachment B but was not properly identified and segregated previously.

56. In the event that a piece of digital media is found not to be (a) an instrumentality of the offense, (b) a fruit of the criminal activity, (c) contraband, or (d) evidence of the offenses specified herein, it will be returned as quickly as possible.

A handwritten signature in black ink, appearing to be a stylized 'J' or 'G' with a loop at the bottom.

AUG 09 2019

CONCLUSION

57. It is the Affiant's belief, based upon the facts contained herein and previous training and experience, that Richard Harvey Olipano Magbanua, did capture and intend to capture images of the private areas of cruise ship passengers and crew under circumstances where the individual had a reasonable expectation of privacy. In creating these videos, it is the Affiant's belief that Magbanua did capture at least one images of a minor in a way and attempted to produce other images of minors in ways that would constitute child pornography and sexually explicit conduct. It is further the Affiant's belief that after producing and attempting to produce child pornography and depictions of minors engaged in sexually explicit conduct, Magbanua did continue to possess those images and depictions on his cellular telephone and transported them onboard the C/S Royal Princess in interstate and foreign commerce and within the special maritime jurisdiction of the United States.

//

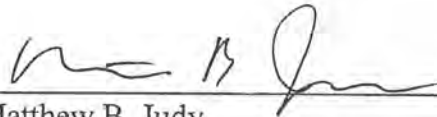
//

//



AUG 09 2019

58. Therefore, it is the affiant's belief, based upon the facts contained herein and previous training and experience, that there is probable cause to believe that evidence, fruits or instrumentalities (see Attachment B, attached hereto and incorporated herein by this reference) of violations of 18 U.S.C. § 1801, § 2251(a), §2252(a)(1), and § 2252(a)(4)(B), are currently concealed within the SUBJECT DEVICE described in Attachment A.


Matthew B. Judy
Special Agent
Federal Bureau of Investigation

electronically *8/9/2019*
telephonically
SUBSCRIBED AND SWORN TO ~~BEFORE ME~~ this 9 day of August 2019, at
Juneau, Alaska.



/S/ MATTHEW M. SCOBLE
U.S. MAGISTRATE JUDGE
SIGNATURE REDACTED

Matthew M. Scoble
United States Magistrate Judge